Exhibit A

Comments of EPIC
RM-10865

DECLARATION

I Edward Hill hereby declare as follows:

1. I am a Special Agent with the Federal Bureau of Investigation, and have been an Agent for 10 years. I specialize in technical equipment, including electronic surveillance equipment. I am familiar with the Internet and with surveillance devices used for the Internet.

2. If authorized by this court, I or other technicians intend to install a program called Carnivore to obtain the information sought in this order. The program will be installed on EarthLink's network, most likely on a "router" used by EarthLink. A "router" is a transmission device that processes packetized network information. Both the router and EarthLink's network are connected to the telephone lines and transmit packetized network information over the telephone lines. The Carnivore software program watches the incoming telephone traffic to EarthLink and looks for the targeted subscriber's log-in name or electronic mail account name. If it finds the target's log-in name, the program follows the target while the target is on line. The program then captures only the header information for electronic mail messages sent or received by the target while the target is on line. If the program finds the target's electronic mail account name, it will capture the header information associated with that electronic mail message. Specifically, the program will capture the time, date, and the addressing information (i.e., Internet identity) for electronic mail messages sent to or from the account. The program will not

capture the subject or regarding line on the electronic mail message, nor does it capture the content of the message or any information concerning the target's other on line activity.

3. Although the program is capable of capturing more than the information authorized under the order, I or the installing technicians will configure the program in a manner that will prevent the program from capturing any information that is not authorized under the order. In addition, the computer used to run the program has limited memory capacity and limited ability to process information. Because of these limitations the computer used to run the program would be overloaded within a few minutes if it attempted to collect all of the information on EarthLink's 8 to 10 million e-mail messages. Moreover, the program will be installed on a particular entry point into EarthLink's network, and as such would not have access to all of EarthLink's customers.

4. The program should not create a security risk for EarthLink. Although the Carnivore program is remotely accessible, it has several security provisions that prevent an intruder from obtaining unauthorized access to EarthLink's system. Even if an intruder did obtain such access, the program lacks a TCP/IP protocol stack, which means that the intruder would be unable to communicate with EarthLink's system from the government's computer. I and other agents with whom I work have installed this program at many other service providers (including AT&T) and have not had security problems or objections from the providers.

5. I have participated in the installation of several pen register and trap and trace devices on Internet electronic mail accounts and am aware of several others.

I declare under the penalty of perjury that the foregoing is true and correct. Executed January 31, 2000 in Quantico, Virginia.

Edward Hill

Exhibit B

Comments of EPIC
RM-10865

b6-1
b7c-1

From: [redacted]
To: BOWMAN, SPIKE (MARION) [redacted]
Date: 4/5/00 5:29PM
Subject: [redacted]

I just received a call from [redacted] at OIPR. To state that she is unhappy with ITOS and the UBL Unit would be an understatement of incredible proportions. I will try to relate what [redacted] thinks has happened with the above named FISA.

[redacted] secured an ELSUR FISA very quickly on [redacted] at the request of [redacted] states that she was assured that the FBI had special software which could do what the FBI said it could do. In fact [redacted] states that the technical people in Quantico approved the FISA language.

The FBI technical people went to install the FBI software a[redacted] to accomplish the electronic surveillance on March 16.

The software was turned on and did not work correctly. The FBI software not only picked up the E-Mails under the electronic surveillance of the FBI's target, [redacted] but also picked up E-Mails on non-covered targets. The FBI technical person was apparently so upset that he destroyed all the E-Mail take, including the take on [redacted] is under the impression that no one from the FBI [redacted] was present to supervise the FBI technical person at the time. Now the FBI technical people want to run a new software experiment at the carrier to see if it works.

b2-2
b6-1
b6-3
b7c-1
b7c-3

[redacted] states that OIPR was never told that the FBI software was experimental. OIPR was informed that it would work. The FBI technical people are still trying to make it work in [redacted], and want to resume the electronic surveillance. The FBI people in [redacted] also want a physical search warrant to pick up the E-Mails from the carrier, which the FBI picked up on the target, but destroyed.

[redacted] informed me that the FBI does not have the authority to resume electronic surveillance until she receives a written explanation of what has happened and she files something with the court. Obviously, she has no intention of securing a search warrant either until this is straightened out.

When you add this story to the FISA mistakes covered in the E.C. I have prepared to go to the field, and which is in NSLU for signature before it goes to [redacted] for his signature, you have a pattern of occurrences which indicate to OIPR an inability on the part of the FBI to manage its FISAs.

[redacted] and [redacted] please see me ASAP.

Thanks
[redacted]

CC: [redacted]

DOC. #5

Exhibit C

Comments of EPIC
RM-10865

[redacted] b6-1 b7c-1

The following sets out some of the legal issues facing DITU as well as some thoughts on ways to proceed. We need your legal guidance in this matter to formulate a reasonable and prudent course of action, as well as a practical working guide for the personnel of DITU and the Field Office personnel involved in Data Intercepts. I am sure there are other issues and ideas, but this may be a good start. Call me to discuss this in more detail. I am willing to travel to your office at FBIHQ or to meet with you here at QT. If you need any clarification of technical concepts etc, you may call SSA [redacted] at 703-[redacted] or SSA [redacted] at 703[redacted]

b6-1 b7c-1

To initiate an intercept on a network or at an ISP, the DITU installs a collection device with appropriate filters set to capture data within the scope of the Court Order or the effective consent of a consenting party. This filtering process, a component of Etherpeek and Carnivore, filters based on TCP/IP standards. On occasion we encounter non-standard implementation of transmission control and Internet protocols within a network or at an ISP. Encountering non-standard implementation has led to inadvertently capturing and processing data outside the Order or Consent.

Issue I

In instances where we encounter non-standard implementation of a protocol which leads to the improper capture of data, two main concerns arise. The first, and of most immediate concern, is the formulation of a guideline to be followed in resolving the matter. This guideline should extend from the DITU personnel who installed and likely discovered the error, through DITU Management representatives, Field Division Case Agents, CDCs, notifications to AUSAs, Motions to Seal. etc.

Issue II

The second issue, critical in efforts to intercept the data under the Court's Order or under consent from a test account, is how FBI technical personnel, such as, Engineers, Computer Programmers and others, may lawful examine the collected data for the sole purpose of determining why the filters failed and what software changes need to be made to bring the collection in line with the scope of the existing Order. We need to look at the data to figure out what is wrong and how to fix it!!!

Issue III

A third issue which we would like you to consider is that we frequently set up user accounts on networks and install data intercept devices to perform a "test tap" under our own consent. This is generally done as a means of verifying that the location on the network and the filter set would be appropriate for an anticipated or existing intercept Order. In the event that we are doing a "test tap" under consent, looking for our own mail, etc, and inadvertently capture something outside our consent, such as another persons mail, what are our options? Is it a violation of TIII if the interception is not intentional and we do not disclose or endeavor to disclose the information to anyone? May we destroy the information and simply not disclose it to anyone?

Issue IV

Random Access Memory RAM

In relation to the "testing" of network placement and filters, it is generally a technical requirement to install the device with appropriate filters set and initiate the capture process. It may be hours or days before a determination can be made as to the functional operation of the collection. During these first few hours or days, the technical representatives of the FBI, Electrical Engineers, Electronics Engineers, Technically Trained Special Agents and others may frequently examine collected data to determine the efficacy of the installation. In relation to the time period from installation to the verification of proper function, the following question is posed for your consideration. Is there a significant legal difference between Random Access Memory (RAM), that which is not retained when power is removed, and of a hard-drive or floppy disk which retains the data. The thought process here in the DITU being that: during the period of time from the installation to the verification of proper function, the data could be directed to remain in RAM and not be forwarded to a permanent media. Technical representatives could then examine the collected data for proper filtering and

assure that the collection is operating within the scope of the Order.

If the collection appears technically correct, it could then be re-directed from RAM to permanent media and the intercept initiated. If not, the data could be examined in RAM by Computer Programmers/Engineers to determine a filtering change or software patch necessary to effect the Court Ordered intercept. The data in RAM would not be retained by the computer on power-off.

By directing collected data to remain only in RAM, we may gain both the ability to troubleshoot installations and to assure that the data is not written to "storage media" nor recoverable from any media.

Exhibit D

Comments of EPIC
RM-10865

4/12/2000

TO: Marcus Thomas
[redacted]

FROM: [redacted]

RE: Internet/E-Mail Intercepts

This is in response to [redacted] E-mail of 4/11 regarding the captioned matter.

b6-1
b7C-1

The following are some preliminary reactions and thoughts. They are not necessarily final legal answers or guidance. They are offered to stimulate further consideration on all of our parts. As was suggested in the E-mail, we all need to sit down in the very near future and take a little time to talk about our intercept approaches, as well as what we must do when they unintentionally go astray.

Background:

We need to start with a few high-level and familiar thoughts, because they form a background and context for the subsequent discussion. As we are all aware and appreciate, electronic surveillance is a very sensitive investigative (and intelligence/counterintelligence) technique.[1] As such, for over 30 years, it has been carefully regulated by and through statutory regimes at both the Federal and State levels -- which regimes, in many instances, contain provisions that are very specific, and which contain dictates that are quite detailed in their procedural/administrative aspects. On its face, the language of these regimes, as written by the Congress, is essentially black and white, and generally is unforgiving: one complies with the statutes or, alternatively, violates them. In enacting these regimes, Congress sought to balance and advance privacy and effective law enforcement. Moreover, given the sensitivity of this technique, electronic surveillance has been the subject of on-going scrutiny by Congressional oversight committees, the press, privacy groups, and the public. In short, there are few, if any, investigative techniques that are (and have been) subjected to such heightened scrutiny. And there are few, if any, investigative techniques that garner (and have garnered in the past) such vehement criticism when errant surveillances or missteps (be they intentional or unintentional) occur.

While, as noted above, the electronic surveillance laws are often specific and detailed in their provisions, generally they do not address the precise aspects of how, technical speaking, the "intercept" is to occur. Congress eschewed doing so because it would be a bad idea to try to delineate all the various potential interception methodologies/approaches. To do so would infringe upon Executive Branch prerogatives in "executing" the laws. And, it would get into sensitive intercept sources and methods, etc. Nevertheless, both the Congress and the courts have

---

[1] While we in our particular area of law enforcement are so close to this matter that we literally live and breathe electronic surveillance, to others (especially those outside of law enforcement), *any electronic surveillance is a big thing!*

an extremely keen interest in making sure that several things are being attended to by the Executive Branch in conducting electronic surveillance searches and seizures: (1) that illegal, unconstitutional searches are not occurring (i.e., that no searches of persons' communications are occurring without probable cause/warrant/emergency); and (2) that the spirit/intent/letter of the electronic surveillance laws (as implementers of constitutional law -- at least to a degree) are being carried out carefully and judiciously. One aspect of this involves the requirement that such surveillances only be approved with high-level departmental approval and with on-going Departmental legal/administrative oversight.

Interceptions of the "Older" Communications Technology

It is probably fair to say that, historically, Congress has been of the opinion (and correctly so) that, for law enforcement, effecting a lawful interception was not a particularly problematic endeavor. Typical wire line service lent itself to reasonably easy segregation of a target's communications to the target line,[2] and thus to concomitantly effecting lawful (and effective technically-targeted) interceptions. With other identifiers (ESNs, MINs, Cap Codes, etc.) being available, accurately targeted interceptions of cellular phones and pagers could likewise be effected by law enforcement. Importantly, Congress understood that, in order to effect accurate interceptions, law enforcement would seek and obtain assistance from electronic communication service providers (ECSPs) and/or others to properly conduct the intercept ("...upon request [of an ECSP, it shall] furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception ... with a minimum of interference with the services [the ECSP is according to] the person whose communications are to be intercepted"). 2518 U.S.C. 2518(4). Until 1994 (*see* below), there is no clear indication, in the statutes or otherwise, that Congress ever understood *interception accuracy* to be an issue for law enforcement.

Where potential "over-acquisitions" could arise, Congress, privacy groups, and others have homed in and taken an interest. For example, with regard to pen register/DNRs, Congress and others have been concerned about certain (but not all) post cut-through dialing -- i.e., certain dialing that arguably constitutes a substantive communication -- even though related to the target individual (as opposed to communications of others). In this regard, Congress, as part of the CALEA legislation, specified in 18 U.S.C. 3121(c) that law enforcement "shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing or signaling information utilized in call processing." Similarly, under CALEA's assistance capability requirements, Congress specified, as a statutory requirement as part of the interception capability, that telecommunications carriers meet their obligation "in a manner that

---

[2] One possible exception being "party-line" service, which by now is pretty rare. Its unclear exactly what Congress would think about such party-line-related intercepts. Presumably, minimization could be employed to parse the target subscriber's calls. But, at the end of day, under the statutory regime/language, the telephonic communications being targeted for interception would, in fact, be occurring over the properly-targeted telephone line/facility. Here, law enforcement would, at least, be on the correct line/facility that had been authorized for interception by the court.

protects ... the privacy and security of communications and call-identifying information not authorized to be intercepted...." 47 U.S.C. 1002(a)(4)(A).

Internet and E-mail Service Providers

Both Internet Service Providers (ISPs) and E-mail service providers are comprehended within the term "providers of 'electronic communication service'" under the ECPA and Title III/FISA. *See, e.g.,* 18 U.S.C. 2510(15). Moreover, certain facets of E-mail/ISP service, at least with regard to the acts of transmitting and routing wire/electronic communications, can also constitute activity of a "telecommunications carrier," thereby subjecting the communications/carrier to the provisions of CALEA. *See* 47 U.S.C. 1001(8). Accordingly, certainly under the ECPA/Title III/FISA (and perhaps under CALEA), such electronic communication service providers are mandated to afford all the necessary assistance to properly effectuate an interception of electronic communications. Consequently, whenever there is an electronic surveillance order, and whenever there are any questions about "standard/non-standard transmission control(s)," "protocols," or any other technical information matter of consequence in properly and accurately effecting electronic surveillance, these service providers are duty-bound to work with us in properly and lawfully effecting the surveillance order.

Internet/E-mail Interceptions

In the referenced DITU E-mail, it is explained that certain Etherpeek and Carnivore "filters" are utilized to (hopefully) capture data (and only that data) authorized for interception in an electronic surveillance order or pursuant to consent. The E-mail mentions that, on occasion, when non-standard implementations have been encountered, data outside the court order or consent have been captured and processed inadvertently. DITU then presents several issues for examination. In the first two, DITU (1) seeks guidance as to formulating guidelines for reacting to such inadvertent interceptions and (2) whether additional examination of such non-authorized data is permitted to remedy the errant collection/filtering efforts.

As noted in the background comments, the electronic surveillance statutes speak at a rather high level, and are essentially black and white in nature -- with one either complying with the law or facially violating it. The Title III statutes, generally speaking, are not "specific intent" statutes. That is, one does not need to have *special* or *particular bad intention* or *motive* to facially violate the law. Further, since the protection of personal communications privacy is a key facet of the statutory purpose and regime, any unauthorized interception of another's communications is a matter of concern (at a minimum). Indeed, some might argue that the government's unauthorized interception of such communications is even more problematic.

Historically, as a matter of Departmental practice/policy, unauthorized interceptions (be they of the subject of the interception or others) have been taken seriously by DOJ (and by the FBI for that matter). When detected, DOJ has advised AUSAs to (1) file a pleading with the court explaining the unintentional/intentional act and to (2) seal the unauthorized intercepted communications with the court, in order to prevent further harm such as subsequent use or disclosure (*see* 18 U.S.C. 2511(1)(c)(d), 2515). Such unauthorized interceptions not only can

violate a citizen's privacy but also can seriously "contaminate" ongoing investigations. In addition, DOJ could also counsel the AUSA to recommend/not recommend to the court whether or not the person(s) who communications were improperly intercepted should be notified.

Interestingly, under Section 2511(2)(a)(ii), while Title III specifies that "no [criminal] cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification [under Title III]," there is no similar explicit protection for law enforcement personnel under this provision. Now, practically speaking, there is virtually no chance that law enforcement officers acting in good faith, pursuant to a court order, are going to be criminally prosecuted (or even investigated)! As to civil liability, under 18 U.S.C. 2520(d), Title III states that "a good faith reliance on ... a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization... is a complete defense against any civil or criminal action brought under [Title III] or any other law." So, here too, law enforcement personnel should be immune, practically speaking, from any liability. (Further, even if (in a semi-egregious case) liability were to be found, it would almost certainly fall to the agency -- not the agent/support personnel.) However, the FBI itself routinely does conduct OPR-type inquiries, from an administrative perspective, in order to determine the nature/cause, etc. of any investigative missteps or errors which facially violate a law, with an eye toward preventing future reoccurrences, etc.

In a similar fashion, missteps under FISA lead to mandatory reporting to the President's Foreign Intelligence Advisory Board (PFIAB), and such errancies must be reported/explained/justified to Congress.

Issue #1:

In short, then, as to the first issue, upon detecting an inadvertent, unauthorized (unlawful) interception:

A) the technical effort that is causing the mistake should be stopped immediately (and not re-instituted until advised to do so by the supervising attorneys);
B) the error should be reported immediately to the FBI substantive case personnel in the field/headquarters (as appropriate), to the field office TA and CDC, and to the respective AUSA/OIPR supervisory attorney (who, in turn, will presumably advise the court);
C) the reporting as to the errant interception should be careful and clear so that those to whom it is reported will fully understand what happened; the reporting should not include any substantive aspect of the *content* of the communication that may have been gleaned; and
D) the unauthorized intercepted material should be segregated immediately as a prelude to formal sealing with the court.

Issue #2:

As to "examining" the unauthorized intercepted data (albeit for the sole purpose of determining why the filters failed and what changes need to be made), this is a very delicate and potentially

problematic area. It would appear that continuing to look at (examine and "use") the substantive content/plain text of the material that was not authorized for interception would most aggravate Title III's concerns/dictates (*see* Sections 2511 and 2515), and most likely would *heighten* the legal problem in the minds of the Department, FBI-OPR, the court, Congress, privacy groups, the public, etc. If, on the other hand, there is some way of looking at the signaling, programing, protocols, etc. *in a raw/unintelligible state (I can amplify later)*, this might be okay if (1) it is for the sole purpose of determining why the filters failed and what changes need to be made, and if (2) it is approved by the AUSA/OIPR (and/or the court if the AUSA/OIPR believe warranted -- such court permission in this area would presumably be preferable from the perspective of legal protection for our technical people). Another thought I would strongly encourage is to engage the ISP. That is, if there is a technical (filter) failure problem regarding the interception, it would appear to be much much more preferable for the ISP to try to fix it (even with us coaching and/ or guiding technically from afar). The reason for fully utilizing the ISP is the existing mandate for their assistance, etc. under the law, and because of the "cover" it affords us legally, politically, and perceptionally.

Issue #3:

DITU poses a similar issue as to one its own "test" accounts where an inadvertent, unauthorized interception occurs. Again, we have to be very careful here, even where "testing" is our activity, because the potential harm/violation of privacy is arguably the same. Somehow, when we test, we have to go out of our way to avoid tripping over innocent third party communications. I am not sure how we can proceed to test without inadvertently intercepting the communications of others, but we really need to try. Perhaps, we can explain our testing requirement to the ISP and get them to test our filters, etc. for us, since it is *their* network, and since *they* administrate it, etc. anyway. I would really encourage using the ISPs for many reasons, not the least of which is to make them aware of us popping around in their network to conduct testing, etc.

Issue #4:

DITU asks whether interception collections effected in Random Access Memory (RAM) (rather than permanent media) make any significant legal difference. In short, I would say probably not as a purely legal matter, inasmuch as an unauthorized interception is, after all, an unauthorized interception. Now, having said that, it may make some feel better that the potential for ongoing "use" and "disclosure"(through some permanent storage media) may be somewhat reduced -- but I don't think this is the path to take. As alluded to above, I would opt for more controlled testing and utilizing service providers as much as possible to create some insulation between us and the subscriber public where inadvertent interceptions might arise in the course of our trying out our filters, etc.